1. Let $\zeta$ be a primitive $n$th root of unity.
   (a) Show that $\zeta^n - 1 \in \mathbb{Q}[x]$ has $n$ distinct roots.
   (b) Write $\mu_n$ for the set of roots of this polynomial. Show that it forms a cyclic group of order $n$.

DEF $\mu_n$ is called the group of roots of unity of order $\mid \text{dividing} \mid n$. A root of unity $\zeta \in \mu_n$ is called primitive if it is a generator, that is if it has order exactly $n$. We write $\zeta_n$ for a primitive root of unity of order $n$, for example $e^{2\pi i/n} \in \mathbb{C}$ (by problem 6(a) the choice doesn’t matter). For the purpose of the problem set we also write $P_n \subset \mu_n$ for the set of primitive roots of unity of order $n$. The polynomial $\Phi_n(x) = \prod_{\zeta \in P_n} (x - \zeta)$ is called the $n$th cyclotomic polynomial. The field $\mathbb{Q}(\zeta_n)$ is called the $n$th cyclotomic field.

(c) Show that $\prod_{d|n} \Phi_d(x) = x^n - 1$. We’ll later show that this is the factorization of $x^n - 1$ into irreducibles in $\mathbb{Q}[x]$.

2. (Prime power and prime order) Fix an odd prime $p$ and let $r \geq 1$.
   (a) Show that $\Phi_{p^r}(x) = \frac{x^{p^r} - 1 - 1}{x - 1}$ and that this polynomial is irreducible.
   (b) Show that $\text{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}) \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times$.
   (c) Show that $\text{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q})$ is cyclic.
   (d) Show that $\mathbb{Q}(\zeta_{p^r})$ has a unique subfield $K$ so that $[K : \mathbb{Q}] = 2$.
   (e) Let $G = \text{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q})$. Show that there is a unique non-trivial homomorphism $\chi: G \to \{ \pm 1 \}$.
   (f) Let $g = \sum_{\sigma \in G} \chi(\sigma) \sigma(\zeta_p)$ (the “Gauss sum”). Show that $g \in K$, $g \notin \mathbb{Q}$, but $g^2 \in \mathbb{Q}$.
   (*g) Show that $g^2 = (-1)\frac{1}{p-1} \frac{1}{p}$, giving a different proof that $K = \mathbb{Q}(g)$.

Examples

3. (Quadratic extension) Let $L = K(\sqrt{d})$ be a quadratic extension of characteristic not equal to 2.
   (a) Write down the matrix of multiplication by $\alpha = a + b\sqrt{d} \in L$ in the basis $\{1, \sqrt{d}\}$.
   (b) Find the trace and determinant of this matrix.
   (c) Let $\sigma$ be the non-trivial element of $\text{Gal}(L/K)$. Show that the answers to (b) agree with $\alpha + \sigma(\alpha)$, $\alpha \sigma(\alpha)$ respectively.
   (RMK Meditate on the case $L = \mathbb{C}$, $K = \mathbb{R}$.)

4. (Cyclotomic extension) Let $\zeta_p$ be a primitive root of unity of order $p$ and equip $\mathbb{Q}(\zeta)$ with the basis $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$. Let $G$ be the cyclic group $\text{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$.
   (a) Write down the matrix of multiplication by $\zeta_p$ in this basis.
   (b) Find the trace and determinant of this matrix.
   (*c) Find its characteristic polynomial.
   (*d) Explicitly compute $\sum_{\sigma \in G} \sigma(\zeta_p)$ and $\prod_{\sigma \in G} \sigma(\zeta_p)$ and show that they equal your answers from parts (b),(d).

Lior Silberman’s Math 501: Problem Set 8 (due 13/11/2020)

(From PS7) Example: Cyclotomic fields
The trace

When \( L/K \) is a finite Galois extension and \( \alpha \in L \) we encounter in class the combination ("trace")

\[
\text{Tr}_K^L(\alpha) = \sum_{\sigma \in \text{Gal}(L/K)} \sigma \alpha,
\]

which we need to be non-zero. We will study this construction when \( L/K \) is a finite separable extension, fixed for the purpose of the problems 5-7.

5. Let \( N/K \) be a finite normal extension containing \( L \).
   (a) For \( \alpha \in L \) we provisionally set
   \[
   \text{Tr}_K^L(\alpha) = \sum_{\mu \in \text{Hom}_K(L,N)} \mu \alpha
   \]
   "trace of \( \alpha \)"
   \[
   N_K^L(\alpha) = \prod_{\mu \in \text{Hom}_K(L,N)} \mu \alpha
   \]
   "norm of \( \alpha \)"
   Where the sum and product range over all \( K \)-embeddings of \( L \) in \( N \). Show that the definition is independent of the choice of \( N \).
   (b) Making a judicious choice of \( N \) show that the trace and norm defined in part (a) are elements of \( K \).
   (c) Show that when \( L/K \) is a Galois extension the definition from part (a) reduces to the combination used in class.

6. (Elements of zero trace) In the application in class we are interested in \( L_0 = \{ \alpha \in L \mid \text{Tr}_K^L(\alpha) = 0 \} \).
   (a) Show that \( \text{Tr}_K^L : L \to K \) is a \( K \)-linear functional on \( L \), so that \( L_0 \) is a \( K \)-subspace of \( L \).
   (b) When \( \text{char}(K) = 0 \), show that \( L = K \oplus L_0 \) as vector spaces over \( K \) (direct sum of vector spaces; the analogue of direct product of groups). Conclude that when \( [L : K] \geq 2 \) the set \( L_0 \setminus K \) is non-empty.
      (e.g. the normal closure).
   (c) Show that \( \text{Tr}_K^L \) is a non-zero linear functional in all characteristics.
   (d) Show that \( L_0 \) is not contained in \( K \) unless \( [L : K] = \text{char}(K) = 2 \), in which case \( L_0 = K \), or \( [L : K] = 1 \) in which case \( L_0 = \{0\} \).

7. (Yet another definition) We continue with the separable extension \( L/K \) of degree \( n \).
   (a) Let \( f \in K[x] \) be the (monic) minimal polynomial of \( \alpha \in L \), say that \( f = \sum_{i=0}^d a_i x^i \) with \( a_d = 1 \).
      Show that \( \text{Tr}_K^K(\alpha) = -a_{d-1} \) and that \( N_K^K(\alpha) = (-1)^{d}a_0 \).
      \( \text{Hint} \): Recall the proof that \( [L : K] \) has \( n \) embeddings into a normal closure.
   (b) Show that \( \text{Tr}_K^L(\alpha) = -\frac{1}{n}a_{d-1} \) and that \( N_K^L(\alpha) = (-1)^n a_0^{n/d} \).
     \( \text{Hint} \): Show that we have \( L \simeq (K(\alpha))^{n/d} \) as \( K(\alpha) \)-vector spaces.

   Definition. From now on we define the trace and norm of \( \alpha \) as in 7(c). Note that this definition makes sense even if \( L/K \) is not separable.

8. (Transitivity) Let \( K \subseteq L \subseteq M \) be a tower of finite extensions. Show that
   (a) \( \text{Tr}_K^M = \text{Tr}_K^L \circ \text{Tr}_L^M \).
   (b) \( N_K^M = N_K^L \circ N_L^M \).
Supplementary problems

A. (Purely inseparable extension) Let $L/K$ be an purely inseparable algebraic extension of fields of characteristic $p$.

(a) For every $\alpha \in L$ show that there exists $r \geq 0$ so that $\alpha^{p^r} \in K$. In fact, show that the minimal polynomial of $\alpha$ is of the form $x^{p^r} - \alpha^{p^r}$.

*Hint:* Consider the minimal polynomials of $\alpha$ and $\alpha^p$.

(b) Conclude that when $[L : K]$ is finite it is a power of $p$.

(c) When $[L : K]$ is finite show that $\text{Tr}_{L/K}$ is identically zero.

B. Let $L = \mathbb{C}(x)$ (the field of rational functions in variable) and for $f \in L$ let $(\sigma(f))(x) = f(\frac{1}{x})$, $(\tau(f))(x) = f(1-x)$.

(a) Show that $\sigma, \tau \in \text{Aut}(L)$ and that $\sigma^2 = \tau^2 = 1$.

(b) Show that $G = \langle \sigma, \tau \rangle$ is a subgroup of order 6 of $\text{Aut}(L)$ and find its isomorphism class.

(c) Let $K = \text{Fix}(G)$. Find this field explin elements $\alpha \in L$ with trace zero. For this, leticitly.